

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of:

The Use of a Cell-Site Simulator to Locate the Cellular
Device Assigned Call Number [(414) 305-2399])
)
)Case No.23-826M(NJ)
)
)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Wisconsin:

See Attachment A.

I find that the affidavit(s) or any recorded testimony, establish probable cause to search and seize the person or property described above and that such search will reveal:

See Attachment B.

YOU ARE COMMANDED to execute this warrant ON OR BEFORE 1/26/2023 (not to exceed 14 days) ☐ in the daytime between 6:00 a.m. and 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph.
(United States Magistrate Judge)☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)
☒ for 30 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.Date and time issued: 1/12/2023 @2:26 p.m.
Judge's signatureCity and State: Milwaukee, WisconsinHonorable Nancy Joseph

, U.S. Magistrate Judge

Return

Case No:	Date and time warrant executed:	Copy of warrant and inventory left with:
----------	---------------------------------	--

Inventory made in the presence of:

Inventory of the property taken and/or name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the undersigned judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

Subscribed, sworn to, and returned before me this date:

Date: _____

United States Magistrate Judge

ATTACHMENT A

This warrant authorizes the use of the electronic investigative technique described in Attachment B to identify the location of the cellular device assigned phone number 414-305-2399, whose wireless provider is Verizon Wireless.

This Warrant also serves as a Pen Register order under 18 U.S.C. § 3123. The Court makes the following findings: James Bernier [XX/XX/1986] is the person to whom the pen register or trap and trace device is to be attached/applied and who is the subject of the criminal investigation; 414-305-2399 is the phone number to which the device is to be attached; and Title U.S.C. § Statute is the offense, or one of the offenses, to which information relates; and

The attorney for the government has certified to this Court that the information likely to be obtained by the installation and use of the pen register or trap and trace device is relevant to an ongoing criminal investigation by the Federal Bureau of Investigation.

ATTACHMENT B

Particular Things to Be Seized with a Cell Site Simulator or Wi-Fi Geolocation Device

This Warrant authorizes the officers to whom it is directed to determine the location of the target cellular device by collecting and examining:

1. radio signals emitted by the target cellular device for the purpose of communicating with cellular infrastructure, including towers that route and connect individual communications; and
2. radio signals emitted by the target cellular device in response to signals sent to it by the officers;

for a period of thirty (30) days, during all times of day and night. This includes monitoring non-content signaling and routing information, including all non-content packet switched data, through the installation and use of a pen register and trap and trace device pursuant to 18 U.S.C. § 3123 by the Federal Bureau of Investigation. Because the use of the device, a Cell Site Simulator or Wi-Fi geolocation device, may fall within the definitions of a “pen register” or a “trap and trace device,” see 18 U.S.C. § 3127(3) & (4), the application and the warrant are designed to comply with the Pen Register Statute as well as Rule 41. The application therefore includes all information required for and serves as a pen register application, 18 U.S.C. § 3123(a); similarly, the warrant therefore includes all the information required for and serves as a pen register order, 18 U.S.C. § 3123(b).

This warrant does not authorize the interception of any content (telephone, text message, or internet based). The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will

be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be the Target Cellular Device, and law enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any information from a cellular device other than the Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices.

Under this warrant, the cell site simulator / geolocation device shall be transferable to any changed dialed number subsequently assigned to a device bearing the same ESN, IMSI, or SIM as the Target Cellular Device; any changed ESN, IMSI, or SIM subsequently assigned the same dialed number as the Target Cellular Device; or any additional changed dialed number, ESN, IMSI, or SIM listed to the same subscriber account as the Target Cellular Device.

The Court finds reasonable necessity for use of the techniques and collection of information described. *See* 18 U.S.C. § 3103a(b)(2).

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the information described. *See* 18 U.S.C. § 3103a(b)(2).

ATTACHMENT B

Particular Things to Be Seized from Device Service Provider

1. Information about the target cell phone and its location, later referred to collectively as location information, includes all precision location information, E-911 Phase II data, GPS data, latitude-longitude data, per call measurement or timing advance data (RTT, True Call, LDBoR, or equivalent), and real time cell site information for 30 days beginning from the date the warrant was issued. This includes initiating a signal to determine the location of the target cell phone on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times directed by the government. The information includes monitoring non-content signaling and routing information, including all non-content packet switched data, through the furnishing of information, facilities, technical assistance, and the installation and use of a pen register and trap and trace device pursuant to 18 U.S.C. §§ 3123-3124 by the service provider and the Federal Bureau of Investigation. Because the request for such location data may include use of a "pen register" or a "trap and trace device," see 18 U.S.C. § 3127(3) & (4), the application and the warrant are designed to comply with the Pen Register Statute as well as Rule 41. The application therefore includes all information required for and serves as a pen register application, 18 U.S.C. § 3123(a); similarly, the warrant therefore includes all the information required for and serves as a pen register order, 18 U.S.C. § 3123(b).
2. All subscriber and extended subscriber information, handset identifiers, handset make and model, WI-FI MAC address, and account notes and memos pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. §2703(c).

3. Call detail records and data reports with cell site location information for voice, SMS, MMS, and data connections, originating and destination IP addresses, and per call measurement or timing advance data (RTT, True Call, LDBoR, or equivalent) for the past thirty (30) days pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. §2703(c).

4. To the extent that the information described is within the possession, custody, or control of the service provider, the service provider is required to disclose all location information to the government and provide all technical assistance necessary to accomplish the collection of the location information unobtrusively and with as little interference as possible.

5. This pen register / trap and trace device shall be transferable to any changed dialed number subsequently assigned to a device bearing the same ESN, IMSI, or SIM as the Target Cellular Device; any changed ESN, IMSI, or SIM subsequently assigned the same dialed number as the Target Cellular Device; or any additional changed dialed number, ESN, IMSI, or SIM listed to the same subscriber account as the Target Cellular Device.

6. The government shall compensate the service provider for reasonable expenses incurred in furnishing such facilities or assistance. Any service provider or representative who gains access to the information in this warrant shall not disclose the existence of the warrant, order, or investigation to any third party unless ordered to do so by the Court. Additionally, the agency requests that all court orders and supporting documents, including the affidavit and search warrant, be sealed until further order by the Court.

7. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the information described. *See* 18 U.S.C. § 3103a(b)(2).

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

In the Matter of the Search of:

The Use of a Cell-Site Simulator to Locate the Cellular
Device Assigned Call Number [(414) 305-2399]

)
)
)Case No. 23-826M(NJ)
)
)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:

18 U.S.C. 2251(a)	Attempted production of child pornography
18 U.S.C. 2252(a)(2)	Receipt/distribution of child pornography
18 U.S.C. 2252(a)(4)(B)	Possession of child pornography

The application is based on these facts: See Affidavit in Support of an Application for a Search Warrant. To ensure technical compliance with the Pen Register Statute, 18 U.S.C. §§ 3121-3127, this warrant also functions as a pen register order. Consistent with the requirement for an application for a pen register order, I certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [investigative agency].

- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

ABBEY MARZICK
Digitally signed by ABBEY MARZICK
Date: 2023.01.11 14:22:06 -06'00'

Applicant's signature

Abbey M. Marzick, Assistant United States Attorney
Printed Name and Title

Sworn to before me and signed via telephone:

Date:

1/12/2023

Nancy Joseph
Judge's signature

Honorable Nancy Joseph, U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel Gartland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c) to authorize law enforcement to employ electronic investigative techniques, as described in the following attachment, to determine the location of the target cellular device assigned dialed number 414-305-2399, referred to in this affidavit as the "Target Cellular Device." The service provider for the target cellular device is Verizon Wireless. This affidavit is made in support of up to two different search warrants to locate the phone: 1) by obtaining information from the service provider, e.g., cell site and other precision location information and/or 2) by utilizing a device that acts as a cell phone tower sometimes referred to as a Cell Site Simulator or Wi-Fi geolocation device. In addition, because this request may be construed as a Pen Register / Trap and Trace device or request, the application for this warrant (which includes this affidavit) is intended to comply with 18 U.S.C. § 3122.

2. I am a Special Agent, (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2018. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search and arrest warrants. I am currently assigned to the FBI Milwaukee Division and am a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. I am authorized to investigate violent crimes against children, to include the possession, production, and distribution of child sexual abuse material (commonly known as "CSAM"). I have experience in the investigation,

apprehension and prosecution of individuals involved in federal criminal offenses, specifically related to the exploitation of children. I have investigative experience and training in the use of cellular devices to commit those offenses and the available technology that can be used by law enforcement to assist in identifying the users of cellular devices and their location.

3. The facts in this affidavit come from my personal observations, training, experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. There is reason to believe the target cellular device is currently located in this district. The believed user of the Target Cellular Device provided the telephone number associated with the device to the Milwaukee Police Department on or about December 21, 2022.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that James Bernier [XX/XX/1986] is using the Target Cellular Device. I know from training and experience that cell phone users normally have their cell telephones with them, so locating a user's cell phone will show that user's location. I believe that locating the Target Cellular Device will constitute and lead to evidence of federal offenses, namely Title 18 United States Code § 2251(a), attempted production of child pornography, Title 18 United States Code § 2252(a)(2), receipt/distribution of child pornography, and Title 18 United States Code § 2252(a)(4)(B), possession of child pornography, committed by James Bernier [XX/XX/1986]. Further, I believe the Target Cellular Device itself will contain evidence of such federal offenses.

DEFINITIONS

6. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. “Child Pornography” is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. An “Internet Protocol address” (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

e. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

f. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

h. “Visual depictions” include undeveloped film and videotape, and data stored on a computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

i. “Website” consists of text pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol.

BACKGROUND ON DISCORD

7. Discord is a messaging platform where millions of users from around the world connect with each other through chat, voice, and video. Discord has both a desktop (PC, Mac, Linux) application and a mobile (iOS, Android) application, and the service can also be accessed from the website directly at www.discordapp.com.

8. In order to use the services, users need to create an account by selecting a username. Once they've made their account, users can create a server and invite their friends to join it with an invite link, or they can join an existing server. Servers are broken down into sub-categories or "channels" where users can connect with each other by either chatting or calling. Users can also communicate through direct messages, which are private chats created between 1-10 users.

9. To create a Discord account, the user is also required to provide an email address which is verified by Discord.

10. Providers like Discord, Inc. typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the SUBJECT ACCOUNT.

11. In some cases, Discord users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

12. On or about September 21, 2022, FBI Kansas City received a report of a subject engaged in the production of child sexual abuse material (CSAM). The subject, Eduardo Gonzales, was identified as a family friend who had sexually abused the complainant's 17-year-old daughter (Victim 1) since she was in approximately the sixth grade.

13. On or about September 22, 2022; Victim 1 was interviewed and disclosed that Gonzales would force Victim 1 to dress in different lingerie and then Gonzales would take pictures of Victim 1.

14. On or about September 22, 2022, Gonzales was interviewed, and admitted that he bought Victim 1 lingerie and would then take pictures of her wearing it. Gonzales disclosed that this then progressed to Gonzales taking naked pictures of Victim 1. Gonzales also disclosed that Gonzales operated a Discord account where Gonzales pretended to be Victim 1 in order to "catch" other users who were interested in underage girls.

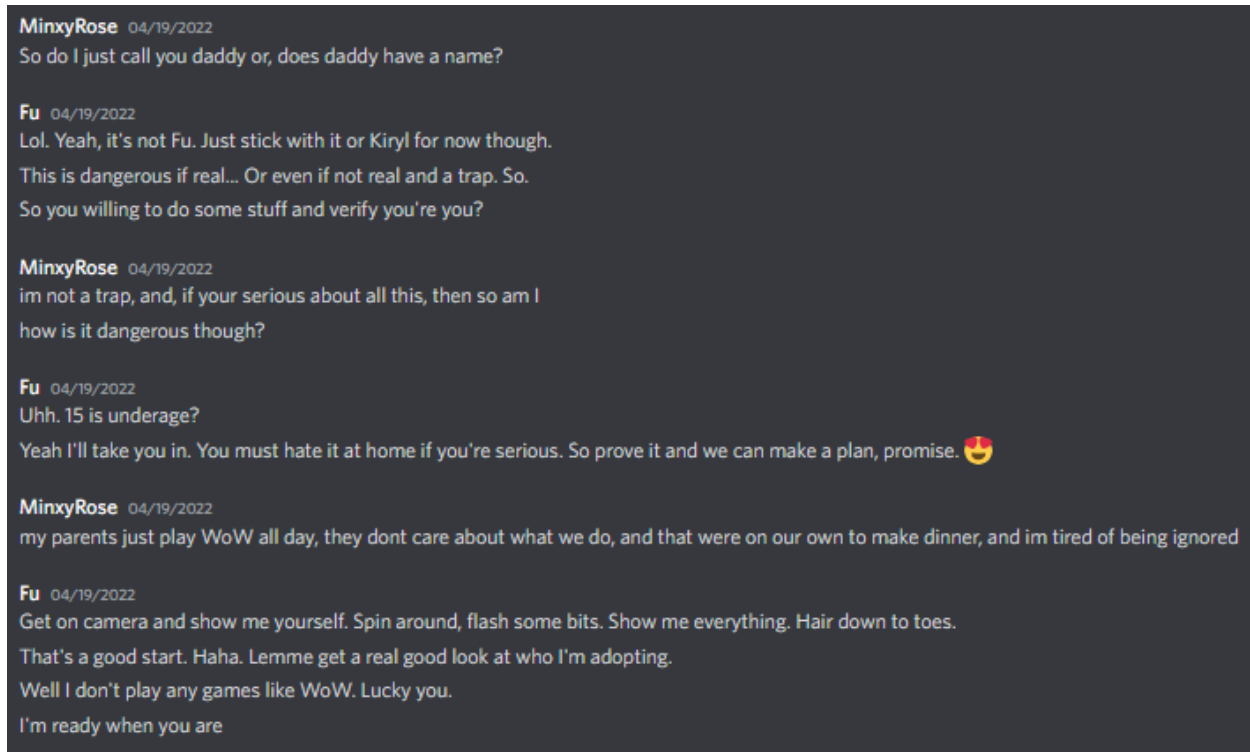
15. On or about September 22, 2022, Gonzales provided written consent for FBI Kansas City to assume his online identity pertaining to multiple accounts. This included Gonzales' Discord account, "MinxyRose#0054" (hereinafter "MinxyRose"). This is the account that Gonzales used when he pretended to be Victim 1.

16. On or about October 4, 2022 an FBI Task Force Officer, operating in an online undercover capacity, (hereinafter “FBI-OCE”), logged into the Discord account MinxyRose and directed his investigative focus to Discord user “Fu#9282” (hereinafter the “SUBJECT ACCOUNT”) because the SUBJECT ACCOUNT was identified as an account exchanging CSAM and discussing possibly meeting MinxyRose, who the user of the SUBJECT ACCOUNT believed to be 15 years old.

17. The conversation between MinxyRose and the user of the SUBJECT ACCOUNT, that FBI-OCE was able to see once he logged on, started on or about April 19, 2022. At that time, Gonzales was operating the MinxyRose account. It is not known at this time if there were any prior communications between the two accounts.

18. On or about April 19, 2022, the SUBJECT ACCOUNT sent a message to MinxyRose which stated, “much better here than rph.” I know from my review of the Discord search warrant material that the SUBJECT ACCOUNT was a member of a group called “Role Play Haven.” This appears to show that the user of the SUBJECT ACCOUNT and MixyRose met in that group, although it is still not known if there were any prior communications. Despite being in a “role play” group, the user of the SUBJECT ACCOUNT, as shown in the next paragraph states “this is dangerous if real,” and as described in subsequent paragraphs requests, sends, and possesses images consistent with CSAM.

19. On or about April 19, 2022, the following chat exchange took place between Gonzales as MinxyRose, and the user of the SUBJECT ACCOUNT¹:



The screenshot shows a chat interface with a dark background. The messages are as follows:

MinxyRose 04/19/2022
So do I just call you daddy or, does daddy have a name?

Fu 04/19/2022
Lol. Yeah, it's not Fu. Just stick with it or Kiryl for now though.
This is dangerous if real... Or even if not real and a trap. So.
So you willing to do some stuff and verify you're you?

MinxyRose 04/19/2022
im not a trap, and, if your serious about all this, then so am I
how is it dangerous though?

Fu 04/19/2022
Uhh. 15 is underage?
Yeah I'll take you in. You must hate it at home if you're serious. So prove it and we can make a plan, promise. 🍑

MinxyRose 04/19/2022
my parents just play WoW all day, they dont care about what we do, and that were on our own to make dinner, and im tired of being ignored

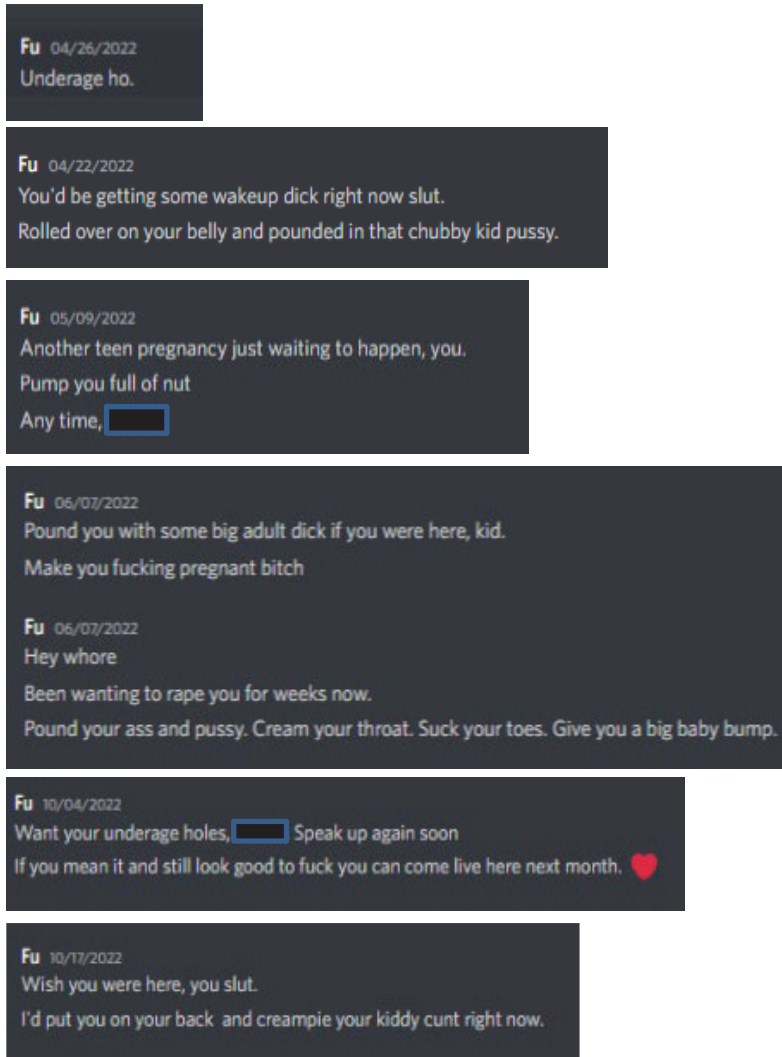
Fu 04/19/2022
Get on camera and show me yourself. Spin around, flash some bits. Show me everything. Hair down to toes.
That's a good start. Haha. Lemme get a real good look at who I'm adopting.
Well I don't play any games like WoW. Lucky you.
I'm ready when you are

20. In these messages, the user of the SUBJECT ACCOUNT is confirming that the user believes MinxyRose to be 15 years old.

21. The user of the SUBJECT ACCOUNT is also requesting that MinxyRose “flash some bits. Show me everything.” Subsequent to that message from the user of the SUBJECT ACCOUNT, MinxyRose sent a video which showed Victim 1, from the waist up, nude and exposing Victim 1’s breasts to the camera.

¹ This is a screen capture of the messages between MinxyRose and Fu taken by FBI-OCE subsequent to the account takeover. No times were shown in the screen capture.

22. On multiple occasions the user of the SUBJECT ACCOUNT made reference to MinxyRose being underage, or a kid. These messages show that the user of the SUBJECT ACCOUNT believed that the user was chatting with a minor. These messages and the date they were sent are below²:



23. On or about May 31, 2022, the user of the SUBJECT ACCOUNT sent three images to MinxyRose. The first two images were sexually explicit images of a female kneeling down with

² The name of Victim 1 was used in the chats, but it has been redacted from these messages to protect the identity of Victim 1.

her buttocks towards the camera and her nude anus exposed. The third image, consistent with the definition of CSAM, showed Victim 1 lying on her back on a bed, her hair in pigtails, nude except for white stockings, with her legs spread and her nude vagina exposed to the camera. After the first image the user of the SUBJECT ACCOUNT sent a message which stated “Fat whore. Knock you the fuck up.” After the third image the user of the SUBJECT ACCOUNT sent a message which stated “Sailor moon³ looking bitch begging for it. What a whore.” During this chat exchange the user of the SUBJECT ACCOUNT sent at least one image consistent with the definition of child pornography.

24. On multiple occasions the user of the SUBJECT ACCOUNT requested that MinxyRose send the user nude images. One example of a message where the user of the SUBJECT ACCOUNT requested nude images is below⁴:

³ Sailor moon is a popular female cartoon character who wore her hair in pigtails.

⁴ The redacted portion of this chat is a zoomed in image of an erect male penis.



25. In another instance while FBI-OCE was operating MinxyRose, MinxyRose told the SUBJECT ACCOUNT that MinxyRose had an 8-year-old stepsister. After this, the user of the SUBJECT ACCOUNT told MinxyRose to take pictures of the 8-year-old. The messages are below:

Fu 10/04/2022
Are you alone?

MinxyRose 10/04/2022
no

Fu 10/04/2022
Then duck in the bathroom for a minute. I want to see your body.

MinxyRose 10/04/2022
i havent changed any

Fu 10/04/2022
Then they will be good pictures. ❤️

MinxyRose 10/04/2022
i have a better idea if u interested in my step-sis at all

Fu 10/04/2022
I'm a nasty man who wants to fuck little girls.
What do you think?

MinxyRose 10/04/2022
i want to expose her

Fu 10/04/2022
Then get pictures or video of her too when she's sleeping. Pull bac the covers and show her off

MinxyRose 10/04/2022
what all yuou want to see of her?

Fu 10/04/2022
Anything and everything. Just like you.

26. These chats show that the user of the SUBJECT ACCOUNT, knew that MinxyRose was a minor, received sexually explicit images and videos from MinxyRose, and requested that MinxyRose self-produce further sexually explicit images and videos of MinxyRose and the 8-year-old stepsister.

IDENTIFICATION OF THE SUBJECT

27. On or about September 30, 2022; a Task Force Officer (TFO) with the FBI sent an administrative subpoena to Discord Inc. regarding the SUBJECT ACCOUNT. On or about October 3, 2022, Discord Inc. provided a response to the administrative subpoena. The response

contained a log of IP addresses used to access the SUBJECT ACCOUNT, as well as the verified email address jbernier2005@hotmail.com.

28. On or about November 3, 2022, an FBI Special Agent obtained a search warrant in the Eastern District of Wisconsin for the SUBJECT ACCOUNT and served the search warrant on Discord Inc. On or about November 8, 2022 Discord Inc. provided a response to the search warrant which contained information and content related to the SUBJECT ACCOUNT.

29. In the Discord Inc. search warrant return an FBI Special Agent observed a conversation between the SUBJECT ACCOUNT and another account (ACCOUNT 2). There was no CSAM shared between the SUBJECT ACCOUNT and ACCOUNT 2, however, the user of ACCOUNT 2 regularly referred to the user of the SUBJECT ACCOUNT as “James.” The user of ACCOUNT 2 was paying the user of the SUBJECT ACCOUNT to write game reviews for the user of ACCOUNT 2.

30. In the Discord Inc. search warrant return an FBI Special Agent observed an image sent by the user of the SUBJECT ACCOUNT to ACCOUNT 3, on or about June 29, 2022, which showed a white male, shirtless, with his face partially covered with his hand, taking a picture in a mirror. This male had dark facial hair and appeared to be tall and heavyset. After sending the image the user of the SUBJECT ACCOUNT stated “Gotta hide my face too. Never know.” The nature of the conversation between the SUBJECT ACCOUNT and ACCOUNT 3 was sexually explicit in nature and the user of ACCOUNT 3 described themselves as almost 14 years old. At this time, it is not known how old the user of ACCOUNT 3 actually was, however the user of the SUBJECT ACCOUNT appeared concerned enough to not show the user’s face.

31. In the same conversation the user of the SUBJECT ACCOUNT also described themselves as “Too tall for the door there.” In or about June 2022 ACCOUNT 3 asked the user of

the SUBJECT ACCOUNT how tall the user of the SUBJECT ACCOUNT was. The user of the SUBJECT ACCOUNT responded “Uh. Very tall. You wouldn’t believe it... 6’8”. 6’9” with my boots on?” Per the Wisconsin Department of Transportation BERNIER is 6’8” tall and over 300 pounds. The stature, and facial hair of the male in the image sent to ACCOUNT 3 are consistent with images seen of BERNIER on BERNIER’s Facebook, and LinkedIn profiles as well as BERNIER’s driver’s license photograph.

32. In or about August 2022, the user of the SUBJECT ACCOUNT started a conversation with ACCOUNT 4, which lasted until approximately October 23, 2022. This conversation was sexually explicit in nature, however, the user of ACCOUNT 4 appeared to identify as an adult and the user of the SUBJECT ACCOUNT referred to the user of ACCOUNT 4 as “woman” on multiple occasions.

33. There were at least nine (9) images shared by the user of the SUBJECT ACCOUNT to ACCOUNT 4 which showed clear images of the user’s face. Each of the images showed the same white male with dark hair, with varying amounts of dark facial hair. One image was taken in a mirror, shirtless, with the male’s face visible. The male’s body type matched the shirtless image sent to ACCOUNT 3. The user of the SUBJECT ACCOUNT did not appear to have any reservations about showing his face in this conversation where the user of ACCOUNT 4 did not identify as a child.

34. On or about October 4, 2022, the user of the SUBJECT ACCOUNT told the FBI-OCE, while operating MinxyRose, that it was the user’s birthday. BERNIER’s birthday is October 4, 1986.

35. On or about October 5, 2022; a TFO with the FBI served an administrative subpoena on Charter Communications, Inc. (Charter) for IP addresses associated with the

SUBJECT ACCOUNT. On or about October 10, 2022, Charter provided a response to the subpoena. The service address associated with the requested IP addresses was 1922A North 31st Street, Milwaukee, WI.

36. On or about October 31, 2022, FBI Milwaukee served an administrative subpoena on Verizon Wireless (Verizon) for IP addresses associated with the SUBJECT ACCOUNT on three separate dates and times. On or about November 10, 2022, Verizon provided a response to the subpoena. The response indicated the IP addresses requested were “Natting IP” addresses, which allows for multiple devices to access the internet via the same IP address. Verizon provided a list of devices associated with each “Natting IP” with a telephone number for each device. Each list contained over 250 devices. Two of the three lists contained telephone number 414-305-2399.

37. On or about December 21, 2022, BERNIER was observed at the 1922A North 31st Street, Milwaukee, WI by an FBI Milwaukee TFO. BERNIER told the TFO that his telephone number was 414-305-2399.

38. A search of a law enforcement database indicated service provider of telephone number 414-305-2399 had been Verizon Wireless since February 7, 2022.

39. Based upon the above information there is probable cause to believe that BERNIER is the user of the SUBJECT ACCOUNT.

40. On January 10, 2023, the Milwaukee County Sheriff’s Office informed FBI Milwaukee that BERNIER was evicted from 1922A North 31st Street, Milwaukee, WI on December 29, 2022.

41. Information obtained from this search warrant will be used to attempt to locate James Bernier [XX/XX/1986] and the Target Cellular Device within the next 30 days.

AUTHORIZATION REQUEST & MANNER OF EXECUTION

42. I request that the Court issue the proposed search warrant pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c) and 2711.

43. Because collecting the information authorized by this warrant may fall within the statutory definitions of a “pen register” or a “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), this application and the accompanying warrant are intended to comply with requirements set forth in 18 U.S.C. §§ 3122-3123.

44. In my training and experience, I have learned that cellular phones and other cellular devices communicate wirelessly across a network of cellular infrastructure, including towers that route and connect individual communications. When sending or receiving a communication, a cellular device broadcasts certain signals to the cellular tower that is routing its communication. These signals include a cellular device’s unique identifiers.

45. In my training and experience, I have learned that Verizon Wireless is a company with its headquarters located within the United States and provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of cellular devices to which they provide service. That information includes (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, (2) cell-site data, also known as “tower/face information” or cell tower/sector records, and (3) timing advance or engineering data commonly referred to as per call measurement data (RTT, True Call, LDBoR, or equivalent). E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device’s signal using data from several of the provider’s cell towers. Cell-site data identifies the “cell towers” (i.e., antenna towers

covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device.

46. To facilitate execution of this warrant, law enforcement may use an investigative device or devices (sometimes referred to as a Cell Site Simulator or Wi-Fi geolocation device) capable of broadcasting signals that will be received by the Target Cellular Device or receiving signals from nearby cellular devices, including the Target Cellular Device. Such a device may function in some respects like a cellular tower, except that it will not be connected to the cellular network and cannot be used by a cell phone to communicate with others. The device may send a signal to the Target Cellular Device and thereby prompt it to send signals that include the unique identifier of the device. Law enforcement may monitor the signals broadcast by the Target Cellular Device and use that information to determine the Target Cellular Device’s location, even if it is located inside a house, apartment, or other building.

47. The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be the Target Cellular Device, and law enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any information from a cellular device other than the

Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices.

48. I request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the target cellular device would seriously jeopardize the ongoing investigation. Such disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). There is a reasonable necessity for the use of the techniques described. *See* 18 U.S.C. § 3103a(b)(2). As further specified in the attachment, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is a reasonable necessity for that seizure. *See* 18 U.S.C. § 3103a(b)(2).

49. I further request the following information from the service provider: the installation and use of a pen register trap and trace device, all real-time precision location information, including E-911 Phase II data, GPS data, and latitude-longitude data, real time cell site information, and per call measurement or timing advance data (RTT, True Call, LDBoR, or equivalent) beginning 30 days from the date the warrant is issued.

50. I further request call detail records and data reports (voice, SMS, MMS), including cell site location information, originating and destination IP addresses, per call measurement or timing advance data (RTT, True Call, LDBoR, or equivalent) for the past 30 days.

51. I further request subscriber and extended subscriber information, handset identifiers, handset make and model, Wi-Fi MAC address, and account notes and memos for the target device.

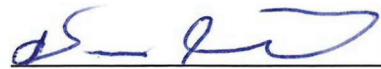
52. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the target cellular device outside of daytime hours.

53. I further request that the pen register / trap and trace device be transferable to any changed dialed number subsequently assigned to a device bearing the same ESN, IMSI, or SIM as the Target Cellular Device; any changed ESN, IMSI, or SIM subsequently assigned the same dialed number as the Target Cellular Device; or any additional changed dialed number, ESN, IMSI, or SIM listed to the same subscriber account as the Target Cellular Device.

54. I further request that the Court order all documents in support of this application, including the affidavit and search warrant, be sealed until further order by the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation. I further request that the Court order any service provider, or their representatives, not to disclose the existence of this warrant or investigation unless ordered to do so by the Court.

55. A search warrant may not be legally necessary to authorize all of the investigative techniques described. Nevertheless, I submit this warrant application out of an abundance of caution.

I declare under penalty of perjury that the foregoing is true and correct and this affidavit was executed in Milwaukee, Wisconsin on January 11, 2023.



Daniel Gartland, Special Agent
Federal Bureau of Investigation

Sworn and subscribed on this 12th day of January, 2023



NANCY JOSEPH
United States Magistrate Judge

ATTACHMENT A

This warrant authorizes the use of the electronic investigative technique described in Attachment B to identify the location of the cellular device assigned phone number 414-305-2399, whose wireless provider is Verizon Wireless.

This Warrant also serves as a Pen Register order under 18 U.S.C. § 3123. The Court makes the following findings: James Bernier [XX/XX/1986] is the person to whom the pen register or trap and trace device is to be attached/applied and who is the subject of the criminal investigation; 414-305-2399 is the phone number to which the device is to be attached; and Title U.S.C. § Statute is the offense, or one of the offenses, to which information relates; and

The attorney for the government has certified to this Court that the information likely to be obtained by the installation and use of the pen register or trap and trace device is relevant to an ongoing criminal investigation by the Federal Bureau of Investigation.

ATTACHMENT B

Particular Things to Be Seized with a Cell Site Simulator or Wi-Fi Geolocation Device

This Warrant authorizes the officers to whom it is directed to determine the location of the target cellular device by collecting and examining:

1. radio signals emitted by the target cellular device for the purpose of communicating with cellular infrastructure, including towers that route and connect individual communications; and
2. radio signals emitted by the target cellular device in response to signals sent to it by the officers;

for a period of thirty (30) days, during all times of day and night. This includes monitoring non-content signaling and routing information, including all non-content packet switched data, through the installation and use of a pen register and trap and trace device pursuant to 18 U.S.C. § 3123 by the Federal Bureau of Investigation. Because the use of the device, a Cell Site Simulator or Wi-Fi geolocation device, may fall within the definitions of a “pen register” or a “trap and trace device,” see 18 U.S.C. § 3127(3) & (4), the application and the warrant are designed to comply with the Pen Register Statute as well as Rule 41. The application therefore includes all information required for and serves as a pen register application, 18 U.S.C. § 3123(a); similarly, the warrant therefore includes all the information required for and serves as a pen register order, 18 U.S.C. § 3123(b).

This warrant does not authorize the interception of any content (telephone, text message, or internet based). The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will

be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be the Target Cellular Device, and law enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any information from a cellular device other than the Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices.

Under this warrant, the cell site simulator / geolocation device shall be transferable to any changed dialed number subsequently assigned to a device bearing the same ESN, IMSI, or SIM as the Target Cellular Device; any changed ESN, IMSI, or SIM subsequently assigned the same dialed number as the Target Cellular Device; or any additional changed dialed number, ESN, IMSI, or SIM listed to the same subscriber account as the Target Cellular Device.

The Court finds reasonable necessity for use of the techniques and collection of information described. *See* 18 U.S.C. § 3103a(b)(2).

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the information described. *See* 18 U.S.C. § 3103a(b)(2).

ATTACHMENT B

Particular Things to Be Seized from Device Service Provider

1. Information about the target cell phone and its location, later referred to collectively as location information, includes all precision location information, E-911 Phase II data, GPS data, latitude-longitude data, per call measurement or timing advance data (RTT, True Call, LDBoR, or equivalent), and real time cell site information for 30 days beginning from the date the warrant was issued. This includes initiating a signal to determine the location of the target cell phone on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times directed by the government. The information includes monitoring non-content signaling and routing information, including all non-content packet switched data, through the furnishing of information, facilities, technical assistance, and the installation and use of a pen register and trap and trace device pursuant to 18 U.S.C. §§ 3123-3124 by the service provider and the Federal Bureau of Investigation. Because the request for such location data may include use of a "pen register" or a "trap and trace device," see 18 U.S.C. § 3127(3) & (4), the application and the warrant are designed to comply with the Pen Register Statute as well as Rule 41. The application therefore includes all information required for and serves as a pen register application, 18 U.S.C. § 3123(a); similarly, the warrant therefore includes all the information required for and serves as a pen register order, 18 U.S.C. § 3123(b).
2. All subscriber and extended subscriber information, handset identifiers, handset make and model, WI-FI MAC address, and account notes and memos pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. §2703(c).

3. Call detail records and data reports with cell site location information for voice, SMS, MMS, and data connections, originating and destination IP addresses, and per call measurement or timing advance data (RTT, True Call, LDBoR, or equivalent) for the past thirty (30) days pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. §2703(c).

4. To the extent that the information described is within the possession, custody, or control of the service provider, the service provider is required to disclose all location information to the government and provide all technical assistance necessary to accomplish the collection of the location information unobtrusively and with as little interference as possible.

5. This pen register / trap and trace device shall be transferable to any changed dialed number subsequently assigned to a device bearing the same ESN, IMSI, or SIM as the Target Cellular Device; any changed ESN, IMSI, or SIM subsequently assigned the same dialed number as the Target Cellular Device; or any additional changed dialed number, ESN, IMSI, or SIM listed to the same subscriber account as the Target Cellular Device.

6. The government shall compensate the service provider for reasonable expenses incurred in furnishing such facilities or assistance. Any service provider or representative who gains access to the information in this warrant shall not disclose the existence of the warrant, order, or investigation to any third party unless ordered to do so by the Court. Additionally, the agency requests that all court orders and supporting documents, including the affidavit and search warrant, be sealed until further order by the Court.

7. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the information described. *See* 18 U.S.C. § 3103a(b)(2).